明 細 書

通信システム、共通鍵制御装置、及び一般通信装置

技術分野

[0001] 本発明は、一般通信装置が保持する共通鍵を新しい共通鍵で更新する技術に関する。

背景技術

[0002] 特許文献1には、暗号化に用いられた共通鍵を特定するために送信データの非暗号化部に共通鍵番号を付与して、送信先の機器へデータを送信する。一方、データを受信した送信先の機器は、受信データに付与されている共通鍵番号からデータを復号化するための共通鍵を選択して復号化する。これにより、送信元及び送信先間において同一の共通鍵を用いた通信を実現し、共通鍵の有効期限の終了時刻に差がある場合において、各機器間で通信ができなくなることを防止し得る機器認証管理システムが開示されている。

特許文献1:特開2003－101533号公報

発明の開示

[0003] しかしながら、特許文献1記載の機器認証管理システムでは、機器は、過去に配信された共通鍵の履歴を保持する必要があった。そのため、上記機器がメモリ容量の小さい白物家電、或いはセンサ等である場合、かかる履歴を保持することは困難であるという問題があった。

[0004] 更に、メモリ容量が小さいため共通鍵の履歴管理を行うことができないという理由で、配信された共通鍵を一つしか持つことができないような機器でネットワークを構成した場合、新たな課題が発生する。

[0005] すなわち、ネットワークに接続される機器が複数存在している場合、全ての機器が保持する共通鍵を更新すると、共通鍵を更新する順番によって、更新後の共通鍵である新共通鍵を保持している機器と更新前の共通鍵である前共通鍵を保持する機器とが混在する期間が発生する。そして、この期間において、新共通鍵を保持する機器と、前共通鍵を保持する機器との間で暗号化したデータによる通信ができなくなると

いう問題が発生する。

[0006] 本発明の目的は、共通鍵を新しい共通鍵で更新する際に、一般通信装置のメモリ消費量を抑制しつつ、全ての一般通信装置間で暗号化したデータを用いて相互に通信することができなくなる期間の発生を防止し得る通信システム、一般通信装置、及び共通鍵制御装置を提供することである。

[0007] 本発明による通信システムは、更新前の前共通鍵を保持する複数の一般通信装置と、前記一般通信装置に対して所定のネットワークを介して接続され、前記前共通鍵を新共通鍵に更新する共通鍵制御装置とを備え、前記共通鍵制御装置は、ステータスが配信完了になった全ての一般通信装置に第1の状態遷移要求を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信するデータ送信処理手段を備え、前記一般通信装置は、前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第1の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第2の状態遷移要求を受信したとき、ステータスを前記移行中から前記更新完了に戻す遷移手段と、ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、ステータスが前記更新完了にあるとき、最新の共通鍵によりデータを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵を用いて送信データを暗号化する暗号化手段とを備えることを特徴とする。

[0008] 本発明による通信システムにおいては、一般通信装置は、共通鍵制御装置から新共通鍵を受信するとステータスを更新完了から配信完了へと遷移させる。ここで、全ての一般通信装置は、新共通鍵を同時に受信することができない。そのため、ネットワークは、ステータスが更新完了である一般通信装置と、ステータスが配信完了である一般通信装置とが混在する状態となる。ここで、説明の便宜上、このネットワークの状態を第1のネットワーク状態と呼ぶことにする。

[0009] この第1のネットワーク状態において、ステータスが配信完了である一般通信装置

は、前共通鍵を用いて送信データを暗号化するが、ステータスが更新完了である一般通信装置は、前共通鍵を保持しているため、当該送信データを復号化することができる。

[0010] また、第1のネットワーク状態において、ステータスが更新完了である一般通信装置は、前共通鍵を用いて送信データを暗号化するが、ステータスが配信完了である一般通信装置は、前共通鍵を保持しているため、前記送信データを復号化することができる。

[0011] 従って、第1のネットワーク状態において、全ての一般通信装置同士は相互に暗号化されたデータを送受信することができる。

[0012] 共通鍵制御装置は、ステータスが配信完了になった全ての一般通信装置に対して第1の状態遷移要求を送信する。第1の状態遷移要求を受信した一般通信装置は、ステータスを配信完了から移行中に遷移させる。ここで、全ての一般通信装置は、第1の状態遷移要求を同時に受信することはできない。そのため、ネットワークは、ステータスが配信完了である一般通信装置とステータスが移行中である一般通信装置とが混在する状態となる。この状態を説明の便宜上、第2のネットワーク状態と呼ぶことにする。

[0013] この第2のネットワーク状態において、ステータスが移行中である一般通信装置は、新共通鍵を用いて送信データを暗号化するが、ステータスが配信完了である一般通信装置は、新共通鍵と前共通鍵とを保持しているため、当該送信データを復号化することができる。

[0014] 一方、ステータスが配信完了である一般通信装置は前共通鍵を用いて送信データを暗号化するが、ステータスが移行中である一般通信装置も新共通鍵と前共通鍵とを保持しているため、当該送信データを復号化することができる。従って、第2のネットワーク状態においても、全ての一般通信装置は相互に通信することができる。

[0015] 共通鍵制御装置は、全ての一般通信装置のステータスが移行中になると、ネットワーク上の全ての一般通信装置に対して第2の状態遷移要求を送信する。第2の状態遷移要求を受信した一般通信装置は、自己のステータスを移行中から更新完了に戻し、前共通鍵を削除する。

[0016] ここで、全ての一般通信装置は、第2の状態遷移要求を同時に受信することができない。そのため、ネットワークは、ステータスが移行中である一般通信装置と、ステータスが更新完了である一般通信装置とが混在している状態となる。ここで、このネットワークの状態を説明の便宜上、第3のネットワーク状態と呼ぶことにする。

[0017] この第3のネットワーク状態において、ステータスが移行中である一般通信装置と、ステータスが更新完了である一般通信装置とは、共に新共通鍵を用いて送信データを暗号化しているため、当該送信データを受信した一般通信装置は、当該送信データを復号化することができる。従って、第3のネットワーク状態においても、全ての一般通信装置は暗号化されたデータを受信することができる。

[0018] その結果、第1～第3のネットワーク状態において、全ての一般通信装置は暗号化されたデータを復号化することが可能となり、しかも、全ての一般通信装置のステータスが更新完了に戻されると、前共通鍵が削除されるため、メモリ消費量を抑制しつつ、全ての一般通信装置が暗号化したデータを用いて相互に通信することができなくなる期間の発生を防止することができる。

図面の簡単な説明

[0019] [図1]本発明の実施の形態による通信システムの全体構成図を示している。

[図2]共通鍵制御装置のブロック構成図を示している。

[図3]一般通信装置のブロック構成図を示している。

[図4]共通鍵更新シーケンスを示す図面であり、(a)は共通鍵更新シーケンスを示し、(b)は一般通信装置のステータスを示し、(c)は一般通信装置が送信データを暗号化する際に使用する共通鍵を示し、(d)は一般通信装置が受信データを復号化する際に使用する共通鍵を示している。

[図5]図2に示す管理テーブルのデータ構造を示した図面である。

[図6]図2に示す共通鍵制御装置のブロック構成図に対して、更に初期共通鍵入力部を追加した場合のブロック構成図を示している。

[図7]本通信システムの具体例を示した図面である。

[図8]本通信システムを実際のホームネットワークに適用した場合のブロック構成図を示している。

発明を実施するための最良の形態

[0020] 以下本発明の実施の形態について、図面を参照しながら説明する。

[0021] 図1は、本発明の実施の形態による通信システムの全体構成図を示している。本通信システムは、共通鍵制御装置11、及び複数の一般通信装置12を備えている。共通鍵制御装置11及び一般通信装置12は、ネットワーク13を介して種々のデータが相互に送受信可能に接続されている。

[0022] 共通鍵制御装置11は、CPU、ROM、RAM、及び通信装置等を備え、一般通信装置12へ共通鍵を送信すると共に、各一般通信装置12に対して送信した共通鍵、各一般通信装置12に対して送信した共通鍵の履歴、及び一般通信装置12のステータス等を管理している。

[0023] ここで、共通鍵とは、通信システムを構成する一般通信装置12及び共通鍵制御装置11が処理するデータを暗号化・復号化する際に用いられるデータである。一般通信装置12のステータスとして、「未設定」、「配信完了」、「移行中」、及び「更新完了」が存在する。

[0024] 「未設定」は共通鍵が共通鍵制御装置11より送信されていない状態を示すステータスである。「配信完了」は、更新対象となる共通鍵である新共通鍵を共通鍵制御装置11から受信したときに遷移するステータスである。「移行中」は共通鍵制御装置11から後述する第1の状態遷移要求を受信したときに遷移するステータスを示す。「更新完了」は共通鍵制御装置11から後述する第2の状態遷移要求を受信したときに遷移するステータスを示す。

[0025] ネットワーク13としては、エコーネット規格に準じたネットワーク、或いはIEEE802.11b(無線LANの一種)の規格に準じたネットワーク、或いはイーサネット(登録商標)の規格に準じたネットワーク等が採用される。

[0026] 図2は、図1に示す共通鍵制御装置11のブロック構成図を示している。共通鍵制御装置11は、通信媒体処理部23、データ受信処理部24、データ送信処理部25、配信共通鍵保持部26、及び共通鍵更新部27を備えている。

[0027] 通信媒体処理部23は、ネットワーク13へ送信データを送信し、ネットワーク13から受信データを受信する。

[0028] データ受信処理部24は、通信媒体処理部23から受信データを受け取った際、配信共通鍵保持部26から当該受信データを暗号化した共通鍵を受け取り、当該受信データを復号化する。

[0029] データ送信処理部25は、配信共通鍵保持部26から送信データの送信先となる一般通信装置12に送信している共通鍵を受け取り、当該送信データを暗号化して通信媒体処理部23へ渡す。但し、データ送信処理部25は、送信先を特定しない、例えばブロードキャストやマルチキャストで送信データを送信する場合、配信共通鍵保持部26から一般通信装置12に対して送信した共通鍵のうち、最新の共通鍵を受け取り、送信データを暗号化して通信媒体処理部23へ渡す。

[0030] 配信共通鍵保持部26は、各一般通信装置12に対して送信した共通鍵の種類を記憶する管理テーブル51を保持する。この管理テーブル51の詳細については後述する。また、配信共通鍵保持部26は、各一般通信装置12に対して送信した全ての共通鍵を保持している。そして、配信共通鍵保持部26は、データ受信処理部24が受信データを受信する際、送信元の一般通信装置12が保持している共通鍵を、管理テーブル51を参照して特定し、特定した共通鍵をデータ受信処理部24へ渡す。

[0031] また、配信共通鍵保持部26は、データ送信処理部25が送信データを送信する際、送信先の一般通信装置12が保持している共通鍵をデータ送信処理部25へ渡す。更に、配信共通鍵保持部26は、通信媒体処理部23が一般通信装置12から共通鍵の更新を要求するデータを受信したとき、送信元の一般通信装置12へ最新の共通鍵が送信されるようにデータ送信処理部25及び通信媒体処理部23を制御する。共通鍵更新部27は、各一般通信装置12が保持する共通鍵を新共通鍵に更新する際、新共通鍵を生成し、各一般通信装置12に送信されるように、データ送信処理部25及び通信媒体処理部23を制御する。

[0032] ここで、共通鍵更新部27は、例えば乱数により共通鍵を生成する。共通鍵を更新するタイミングとしては、例えば以下のタイミングが挙げられる。1)システム使用者が、共通鍵制御装置11の画面や本体から手動で更新を指定したとき、2)前共通鍵による送信データの暗号化回数が一定回数に達したとき、3)前共通鍵による受信データの復号化回数が一定回数に達したとき、4)前共通鍵による送信データの暗号化回

数と前共通鍵による送信データの復号化回数との和が一定回数に達したとき、5)前共通鍵を送信してから一定の時間が経過したとき、6)配信共通鍵保持部26により管理されていない一般通信装置12からデータを受信したとき等が挙げられる。

[0033] 図3は、一般通信装置12のブロック構成図を示している。一般通信装置12は、通信媒体処理部33、データ受信処理部34、データ送信処理部35、共通鍵保持部36、及び共通鍵要求部37を備えている。

[0034] 通信媒体処理部33は、ネットワーク13へ送信データを送信し、受信データをネットワーク13から受信する。データ受信処理部34は、通信媒体処理部33から受信データを受け取ると、共通鍵保持部36から自己のステータスにより定められる共通鍵を受け取り、受信データを復号化する。データ送信処理部35は、共通鍵保持部36から自己のステータスにより定められる共通鍵を受け取り、送信データを暗号化して通信媒体処理部33へ渡す。共通鍵保持部36は、自己のステータスと共通鍵とを保持し、ステータスにより定められる共通鍵をデータ受信処理部34及びデータ送信処理部35へ渡す。

[0035] 具体的には、共通鍵保持部36は、自己のステータスが更新完了である場合、最新の共通鍵のみ保持し、自己のステータスが配信完了及び移行中である場合、新共通鍵と前共通鍵とを保持する。

[0036] 共通鍵要求部37は、電源OFF等によりネットワーク13から離脱していた一般通信装置12がネットワーク13へ参入した際、共通鍵制御装置11に新共通鍵の送信を要求する。これにより、新共通鍵の更新漏れが回避される。

[0037] 本実施の形態では、共通鍵制御装置11のデータ送信処理部25がデータ送信処理手段に相当し、共通鍵更新部27が共通鍵更新手段に相当する。また、一般通信装置12の共通鍵保持部36が遷移手段、及び共通鍵保持手段に相当し、データ送信処理部35が暗号化手段に相当する。

[0038] 図1に示すように、通信システムが複数の一般通信装置12により構成される場合、共通鍵制御装置11が新共通鍵を送信すると、通信システム内には前共通鍵を保持する一般通信装置12と、新共通鍵を保持する一般通信装置12とが混在する。そこで、新共通鍵を保持する一般通信装置12と新共通鍵を保持していない一般通信装

置12と間の通信を可能とするための共通鍵更新シーケンスを図4に示す。

[0039] 図4は、共通鍵更新シーケンスを示す図面であり、(a)は共通鍵更新シーケンスを示し、(b)は一般通信装置のステータスを示し、(c)は一般通信装置が送信データを暗号化する際に使用する共通鍵を示し、(d)は一般通信装置が受信データを復号化する際に使用する共通鍵を示している。

[0040] このシーケンス図の初期状態において、一般通信装置12のステータスは更新完了を示しているものとする。このステータスにおいて、一般通信装置12は、(c)に示すように前共通鍵を用いて送信データを暗号化し、(d)に示すように前共通鍵を用いて受信データを復号化する。

[0041] ステップS1において、共通鍵制御装置11は、全ての一般通信装置12に対して共通鍵更新要求Rを送信する。この共通鍵更新要求Rには新共通鍵が含まれている。ステップS2において、一般通信装置12は、共通鍵更新要求Rを受信し、共通鍵制御装置11に共通鍵更新要求Rに対する応答A1を送信する。このとき、一般通信装置12は、(b)に示すようにステータスを更新完了から配信完了に遷移させる。ここで、ネットワーク13上に存在する全ての一般通信装置12は、共通鍵更新要求Rを同時に受信することができない。そのため、ネットワーク13は、ステータスが更新完了である一般通信装置12と、ステータスが配信完了である一般通信装置12とが混在した状態になる。このネットワークの状態を第1のネットワーク状態J1と呼ぶことにする。

[0042] この第1のネットワーク状態J1において、ステータスが配信完了である一般通信装置12は、(c)に示すように前共通鍵を用いて送信データを暗号化している。そのため、ステータスが更新完了である一般通信装置12は、ステータスが配信完了である一般通信装置12から前共通鍵を用いて暗号化された送信データを復号化することができる。

[0043] 従って、第1のネットワーク状態J1において、ステータスが更新完了である一般通信装置12とステータスが配信完了である一般通信装置12との間で暗号化したデータを送受信することが可能となる。

[0044] ステップS3において、共通鍵制御装置11は一般通信装置12から送信された応答A1を受信する。ステップS4において、共通鍵制御装置11は、全ての一般通信装置

12に共通鍵更新要求Rを送信した後に、応答A1を送信した全ての一般通信装置12に第1の状態遷移要求R1を送信する。

[0045] ステップS5において、一般通信装置12は、第1の状態遷移要求R1を受信すると、(b)に示すようにステータスを配信完了から移行中に遷移させ、第1の状態遷移要求R1に対する応答A2を共通鍵制御装置11に送信する。ここで、ネットワーク13上に存在する全ての一般通信装置12は、第1の状態遷移要求R1を同時に受信することができない。そのため、ネットワーク13は、ステータスが移行中である一般通信装置12とステータスが配信完了である一般通信装置12とが混在した状態となる。このネットワークの状態を第2のネットワーク状態J2と呼ぶことにする。

[0046] この第2のネットワーク状態J2において、ステータスが移行中である一般通信装置12は(c)に示すように新共通鍵を用いて送信データを暗号化しているが、ステータスが配信完了である一般通信装置12は(d)に示すように新共通鍵を保持しているため、当該送信データを復号化することができる。

[0047] また、第2のネットワーク状態J2において、ステータスが配信完了である一般通信装置12は、(c)に示すように前共通鍵を用いて送信データを暗号化しているが、ステータスが移行中である一般通信装置12は、(d)に示すように前共通鍵を保持しているため、当該送信データを復号化することができる。

[0048] そのため、第2のネットワーク状態J2において、ステータスが移行中である一般通信装置12とステータスが配信完了である一般通信装置12とは暗号化されたデータを相互に送受信することができる。

[0049] ステップS6において、共通鍵制御装置11は、一般通信装置12から送信される応答A2を受信する。ステップS7において、共通鍵制御装置11は、全ての一般通信装置12に新共通鍵を配信した場合、第2の状態遷移要求R2を一般通信装置12に送信する。

[0050] ステップS8において、一般通信装置12は、第2の状態遷移要求R2を受信すると、自己のステータスを移行中から更新完了に戻し、共通鍵制御装置11に第2の状態遷移要求R2に対する応答A3を送信する。

[0051] ここで、ネットワーク13上に存在する全ての一般通信装置12は、第2の状態遷移要

求R2を同時に受信することができない。そのため、ネットワーク13上には、ステータスが更新完了である一般通信装置12と、ステータスが移行中である一般通信装置12とが混在している。このネットワークの状態を第3のネットワーク状態J3と呼ぶことにする。

[0052] この第3のネットワーク状態J3において、ステータスが更新完了である一般通信装置12は、(c)に示すように新共通鍵を用いて送信データを暗号化している。そのため、ステータスが更新完了である一般通信装置12は、(d)に示すようにステータスが移行中である一般通信装置12から新共通鍵を用いて暗号化された送信データを復号化することができる。

[0053] また、第3のネットワーク状態J3において、ステータスが移行中である一般通信装置12は、(c)に示すように新共通鍵を用いて送信データを暗号化しているが、ステータスが更新完了である一般通信装置12は、(d)に示すように新共通鍵を保持しているため、当該送信データを復号化することができる。

[0054] そのため、第3のネットワーク状態J3において、ステータスが移行中である一般通信装置12とステータスが配信完了である一般通信装置12とは暗号化されたデータを相互に送受信することができる。

[0055] ステップS9において、共通鍵制御装置11は応答A3を受信する。そして、共通鍵制御装置11が全ての一般通信装置12からの応答A3を受信した場合、ネットワーク13上の全ての一般通信装置12のステータスが更新完了となり、共通鍵の更新処理が終了する。

[0056] なお、一般通信装置が家電機器やセンサ類である場合、共通鍵更新時にネットワークに種々のデータが送受信可能な状態で接続されていない可能性が高い。その場合、共通鍵制御装置11は、一般通信装置12のステータスを更新完了に設定しなくてもよい。

[0057] このように一般通信装置12が保持するステータスに応じて更新シーケンスを実行することによって、共通鍵更新中に新共通鍵に更新された一般通信装置12と新共通鍵に更新されていない一般通信装置12とがシステム内に混在している場合においても、一般通信装置12同士で共通鍵を使用した通信を可能にすることができる。また、

一般通信装置12は、共通鍵配信状態が配信完了状態及び移行中状態のときのみ新共通鍵と前共通鍵とを共に保持し、更新完了状態の場合は最新の共通鍵のみを保持しているため、一般通信装置12がメモリ容量の小さい家電機器やセンサ類であるとしても、対応が可能である。

[0058] 図5は、図2に示す管理テーブル51のデータ構造を示した図面である。図5に示すように、管理テーブル51は、共通鍵の配信履歴を記憶している。管理テーブル51は、共通鍵の種類を示すデータを記憶する共通鍵のフィールドと、各共通鍵を送信した一般通信装置のアドレスを記憶する配信先アドレスのフィールドとを備えている。

[0059] 共通鍵のフィールドには、最新共通鍵、及び共通鍵1～共通鍵nが記憶されている。共通鍵の後に付される1～nの符号は、最新共通鍵に対して何世代前の共通鍵であるかを示す数字であり、例えば共通鍵nは、最新共通鍵に対してn世代前の共通鍵を示している。

[0060] 図5では、アドレスA、アドレスB、アドレスCの一般通信装置12は最新の共通鍵を保持している。アドレスDの一般通信装置12は共通鍵1を保持している。アドレスE、アドレスFの一般通信装置12は、共通鍵2を保持している。共通鍵3を保持する一般通信装置12はシステム内には存在していない。アドレスGの一般通信装置12は共通鍵4を保持している。このように共通鍵制御装置11は管理テーブル51を保持しているため、電源がオフされる等して共通鍵の更新処理が行われていない一般通信装置12に対しても、当該一般通信装置12が保持する共通鍵を用いて暗号化したデータを送信することができる。

[0061] また、管理テーブル51は、各共通鍵と一般通信装置12のアドレスとを対応付けて記憶し、このアドレスは一般通信装置12に対して一意に与えられている。そのため、いずれの一般通信装置12も保持していない共通鍵を格納するためのレコードを保持する必要がなくなる。その結果、この管理テーブル51を不揮発性のメモリに保持させる、或いは揮発性のメモリに登録する保持させる場合であっても、メモリ消費量を低減させることができる。

[0062] 図6は、図2に示す共通鍵制御装置11のブロック図に対して、更に初期共通鍵入力部68を追加した場合のブロック構成図を示している。初期共通鍵入力部68は、管

理テーブル51にアドレスが登録されていない一般通信装置12が保持する共通鍵である初期共通鍵を入力するものである。これにより共通鍵制御装置11は、入力された初期共通鍵を用いて最新の共通鍵を暗号化し、初期共通鍵を保持する一般通信装置12に送信することができる。その結果、最新の共通鍵が第三者によって盗まれることを防止しつつ、最新の共通鍵を一般通信装置12に送信することができる。

[0063] ここで、初期共通鍵入力部68としては、キーボード、タッチパネル、及びマウスが採用される。ただし、これらに限定されず、例えば初期共通鍵を保持する一般通信装置12が家電機器などである場合は、その家電機器のリモコンから送信される信号を受信できる受光部を採用してもよい。この場合、ユーザは家電機器のリモコンを操作して初期共通鍵を入力することができる。

[0064] また、初期共通鍵を保持する一般通信装置12の筐体に製造番号等の符号及びバーコード等がプリントされている場合、或いは一般通信装置12を梱包する箱に製造番号等の符号及びバーコード等がプリントされ、かつこれらの符号及びバーコード等から所定の計算式により初期共通鍵が生成されている場合は、初期共通鍵入力部68として、バーコードリーダー、OCR等の符号を認識する装置を採用し、この装置を用いて符号及びバーコードを読取り、読取った符号及びバーコードを基に、初期共通鍵を生成してもよい。この場合、初期共通鍵入力部68は、上記所定の計算式を予め記憶する必要がある。

[0065] 更に、初期共通鍵入力部68は、例えばSDカード、フレキシブルディスク、CD－R等の記録媒体からデータを読み出す記憶媒体駆動装置を採用してもよい。この場合、記録媒体に初期共通鍵を記憶させておけば、この記録媒体から初期共通鍵を取得することができる。

[0066] 次に本通信システムの具体例を図7に示す。図7に示す通信システムでは、センタサーバ71は、家72の外部に設置されている。共通鍵制御装置11及び一般通信装置12は家72の内部に設置されている。センタサーバ71は共通鍵制御装置11とインターネットを介して接続されている。

[0067] センタサーバ71は、共通鍵制御装置11及び一般通信装置12に関する種々の情報を保持している。まず、初期共通鍵入力部68は、共通鍵の配信先の一般通信装

置12からその一般通信装置12の情報、例えばメーカコード、商品コード、製造番号、製造年月日を取得する。共通鍵制御装置11は、取得したこれらの情報をセンタサーバ71へ送信する。センタサーバ71は、送信されたこれらの情報から予め定められた計算式による演算を実行して初期共通鍵を生成し、共通鍵制御装置11に送信する。これにより、共通鍵制御装置11は、初期共通鍵を取得する。

[0068] 但し、初期共通鍵を取得するためのセンタサーバ71と家72の間で送受信されるデータは、第三者が通信内容を傍受しても判断できないように、暗号化されている必要がある。

[0069] 次に、本通信システムを実際のホームネットワークに適用した場合について図8を用いて説明する。図8に示す通信システムはコントローラ81、エアコン82、及びセンサ83を備えている。コントローラ81は、図1に示す共通鍵制御装置11に相当し、エアコン82及びセンサ83は図1に示す一般通信装置12に相当する。

[0070] センサ83は検知対象物を検知した場合、検知ステータスを有に設定し、エアコン82に対して動作開始要求データを送信する。一方、センサ83は、検知対象物を検知していない場合、検知ステータスを無に設定し、エアコン82に動作停止要求データを送信する。

[0071] まず、エアコン82及びセンサ83の順に共通鍵が更新される場合について説明する。初期状態において、センサ83のステータスは更新完了であり、エアコン82のステータスは配信完了であるものとする。

[0072] この初期状態において、センサ83の検知ステータスが無から有に変化した場合、センサ83は新共通鍵を保持していないため、前共通鍵で動作開始要求データを暗号化して、エアコン82に送信する。このとき、エアコン82のステータスは配信完了であるため、エアコン82は受信した動作開始要求データを新共通鍵で復号化し、暗号化した共通鍵と異なっていることを判断すると、前共通鍵で動作開始要求データを復号化する。その結果、エアコン82はセンサ83から動作開始要求データを受信することができる。

[0073] 次に、センサ83は、コントローラ81から送信される新共通鍵を受信すると、ステータスを更新完了から配信完了に遷移させる。次に、コントローラ81は、エアコン82及び

センサ83に第1の状態遷移要求R1を送信するが、エアコン82が第1の状態遷移要求R1を受信した後であって、センサ83が第1の状態遷移要求R1を受信する前、すなわち、エアコン82のステータスが移行中であり、センサ83のステータスが配信完了である場合、センサ83の検知ステータスが無に変化したとする。このとき、センサ83は、ステータスが配信完了であるため、前共通鍵を使用して動作停止要求データを暗号化してエアコン82に送信する。

[0074] 動作停止要求データを受信したエアコン82は、ステータスが「移行中」であるため、受信した動作停止要求データを新共通鍵で復号化し、暗号化した共通鍵と異なっていることを判断すると、前共通鍵で受信データを復号化する。この結果、エアコン82はセンサ83から動作停止要求データを受信することができる。

[0075] 次に、センサ83は、コントローラ81から第1の状態遷移要求R1を受信してステータスを移行中に遷移させる。次に、コントローラ81は、第2の状態遷移要求R2をエアコン82及びセンサ83に送信し、エアコン82及びセンサ83はこの順で第2の状態遷移要求R2を受信したものとする。そして、エアコン82が第2の状態遷移要求R2を受信した後であって、センサ83が第2の状態遷移要求R2を受信する前、すなわち、エアコン82のステータスが更新完了であり、センサ83のステータスが移行中である場合に、センサ83の検知ステータスが有へ変化したとする。このとき、センサ83は、ステータスが移行中であるため、新共通鍵を使用してエアコン82に動作開始要求データを暗号化して送信する。受信したエアコン82は、ステータスが更新完了であるため、受信した動作開始要求データを新共通鍵で復号化する。この結果、エアコン82はセンサ83から動作開始要求データを受信することができる。

[0076] 次に、センサ83及びエアコン82の順に共通鍵が更新される場合について説明する。初期状態において、エアコン82のステータスは更新完了であり、センサ83のステータスは配信完了であるものとする。

[0077] この初期状態において、センサ83の検知ステータスが有に変化した場合、センサ83はステータスが配信完了であるため、前共通鍵で動作開始要求データを暗号化してエアコン82に送信する。

[0078] エアコン82は受信した動作開始要求データを、保持している前共通鍵で復号化す

る。その結果、エアコン82はセンサ83から動作開始要求データを受信することができる。次に、エアコン82は、コントローラ81から送信される新共通鍵を受信すると、ステータスを配信完了に遷移させる。

[0079] 次に、コントローラ81は、エアコン82及びセンサ83に第1の状態遷移要求R1を送信するが、センサ83が第1の状態遷移要求R1を受信した後であって、エアコン82が第1の状態遷移要求R1を受信する前、すなわち、センサ83のステータスが移行中であり、エアコン82のステータスが配信完了である場合に、センサ83の検知ステータスが無に変化したとする。

[0080] このとき、センサ83はステータスが移行中であるため、新共通鍵を使用して動作停止要求データを暗号化してエアコン82に送信する。受信したエアコン82は、ステータスが配信完了であるため、受信した動作停止要求データを、新共通鍵で復号化し、暗号化した共通鍵と同一であることを確認する。この場合、前共通鍵で受信データを復号化する必要はない。その結果、エアコン82はセンサ83から動作停止要求データを受信することができる。次に、エアコン82は、コントローラ81から第1の状態遷移要求R1を受信して、ステータスを移行中に遷移させる。

[0081] 次に、コントローラ81は、エアコン82及びセンサ83に第2の状態遷移要求R2を送信するが、センサ83が第2の状態遷移要求R2を受信した後であって、エアコン82が第2の状態遷移要求R2を受信する前、すなわち、センサ83のステータスが更新完了であり、エアコン82のステータスが移行中である場合に、センサ83の検知ステータスが無に変化したとする。このとき、センサ83は、ステータスが移行中であるため、新共通鍵を使用して動作停止要求データを暗号化してエアコン82に送信する。

[0082] 動作停止要求データを受信したエアコン82は、ステータスが更新完了であるため、新共通鍵で復号化し、暗号化した共通鍵と同一であることを確認する。この場合、エアコン82は、新共通鍵で受信データを復号化することなく、センサ83から動作開始要求データを受信することができる。

[0083] このような現象は、ホームネットワークのようにM:Nの通信システムにおいて、発生する可能性は十分高い。また、ネットワークが低速の場合においては、共通鍵の更新には、さらに時間も要することとなるが、その場合も常に一般通信装置間において、

通信を行うことが可能である。

[0084] なお、図2に示す各種ブロックは、コンピュータを共通鍵制御装置として機能させるプログラムをCPUに実行させることで実現してもよい。また、図3に示す各種ブロックは、コンピュータを一般通信装置として機能させるプログラムをCPUに実行させることで実現させてもよい。

[0085] (本発明の纏め)

(1)本発明による通信システムは、更新前の前共通鍵を保持する複数の一般通信装置と、前記一般通信装置に対して所定のネットワークを介して接続され、前記前共通鍵を新共通鍵に更新する共通鍵制御装置とを備え、前記共通鍵制御装置は、ステータスが配信完了になった全ての一般通信装置に第1の状態遷移要求を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信するデータ送信処理手段を備え、前記一般通信装置は、前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第1の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第2の状態遷移要求を受信したとき、ステータスを前記移行中から更新完了に戻す遷移手段と、ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、ステータスが前記更新完了にあるとき、最新の共通鍵によりデータを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵を用いて送信データを暗号化する暗号化手段とを備えることを特徴とする。

[0086] この構成によれば、第1～第3のネットワーク状態において、全ての一般通信装置は暗号化されたデータを復号化することが可能となり、しかも、全ての一般通信装置のステータスが更新完了に戻されると、前共通鍵が削除されるため、メモリ消費量を抑制しつつ、全ての一般通信装置が暗号化されたデータを用いて相互に通信することができなくなる期間が発生することを防止することができる。

[0087] (2)上記構成において、前記共通鍵制御装置は、前記新共通鍵を乱数により生成

する共通鍵更新手段を更に備えることが好ましい。

[0088] この構成によれば、新共通鍵は乱数により決定されるため、解読困難な共通鍵を生成することができる。

[0089] (3)上記構成において、前記共通鍵更新手段は、前記前共通鍵による送信データの暗号化回数又は受信データの復号化回数がある一定回数を越えた場合、前記新共通鍵を生成することが好ましい。

[0090] この構成によれば、前共通鍵は使用回数に応じて更新されるため、システムの安全性をより高めることができる。

[0091] (4)上記構成において、前記共通鍵更新手段は、前記共通鍵による送信データの暗号化回数と受信データの復号化回数との和がある一定回数越えた場合、前記新共通鍵を生成することが好ましい。

[0092] この構成によれば、前共通鍵は暗号化回数と復号化回数との和が一定回数を超えた場合に更新されるため、システムの安全性をより高めることができる。

[0093] (5)上記構成において、前記共通鍵更新手段は、前記前共通鍵を更新してからある一定時間経過した場合、前記新共通鍵を生成することが好ましい。

[0094] この構成によれば、前共通鍵は一定期間経過後に更新されるため、システムの安全性をより高めることができる。

[0095] (6)上記構成において、前記共通鍵保持手段は、前記一般通信装置へ送信した共通鍵の履歴を保持し、送信した各共通鍵と、送信した前記一般通信装置のアドレスを含む一般通信装置情報とを対応づけて記憶する管理テーブルを保持することが好ましい。

[0096] この構成によれば、共通鍵保持手段は、各一般通信装置がどの世代の共通鍵を保持しているかを管理しているため、長期間電源がオフされる等して、前共通鍵よりも前の世代の共通鍵を保持する一般通信装置が再び電源がオンされた場合であっても、共通鍵制御装置は当該一般通信装置と送信することができる。

[0097] (7)上記構成において、前記共通鍵更新手段は、前記管理テーブルにより一般通信装置情報が記憶されていない一般通信装置からデータを受信した場合、新共通鍵を生成し、前記管理テーブルにより一般通信情報が記憶されている一般通信装置

が保持する共通鍵を前記新共通鍵に更新することが好ましい。

[0098] この構成によれば、管理テーブルに一般通信情報が記憶されていない一般通信装置がネットワークに接続された場合、全ての一般通信装置に対して最新の共通鍵が送信されるため、各一般通信装置が保持する共通鍵を共通化させることができる。

[0099] (8)上記構成において、前記共通鍵制御装置は、前記一般通信装置がネットワーク接続時において保持する初期共通鍵を入力するための初期共通鍵入力手段を更に備えることが好ましい。

[0100] この構成によれば、一般通信装置がネットワークに組み込まれるときに保持している初期共通鍵を入力する初期共通鍵入力手段を備えているため、共通鍵制御装置がこの初期共通鍵を知らない場合であっても、共通鍵制御装置は当該一般通信装置と通信することができる。

[0101] (9)前記初期共通鍵入力手段は、キーボード、タッチパネル、及びマウスのうちの少なくともいずれか1つを含むことが好ましい。

[0102] この構成によれば、初期共通鍵入力手段は、キーボード、タッチパネル、及びマウス等から構成されるため、ユーザは初期共通鍵を容易に入力することができる。

[0103] (10)上記構成において、前記初期共通鍵入力手段は、初期共通鍵を保持する一般通信装置のリモコンと、前記リモコンからの信号を受け取る受光部とを含むことが好ましい。

[0104] この構成によれば、初期共通鍵の配信先である初期共通鍵を保持する一般通信装置のリモコンを用いて、初期共通鍵を入力することができる。

[0105] (11)上記構成において、前記初期共通鍵入力手段は、符号読取り装置であることが好ましい。

[0106] この構成によれば、一般通信装置の筐体等に記されている、或いは一般通信装置を梱包する袋や箱に記されている初期共通鍵を示す符号を符号読取り装置により読取らせるだけで、初期共通鍵を入力することができる。

[0107] (12)上記構成において、前記初期共通鍵入力手段は、記憶媒体駆動装置でることが好ましい。

[0108] この構成によれば、記録媒体に初期共通鍵が記録されている場合、この記録媒体

を記録媒体駆動装置に装填するだけで、初期共通鍵を入力することができる。

[0109] (13)上記構成において、前記一般通信装置は、通信不可能状態から通信可能状態になったとき、前記共通鍵制御装置に対して新共通鍵の配信を要求するデータを作成し、前記共通鍵制御装置に送信する共通鍵要求手段を更に備えることが好ましい。

[0110] この構成によれば、長期間電源がオフされる等して通信不可能状態にあった一般通信装置が通信可能状態になった場合、共通鍵制御装置に対して新共通鍵の送信を要求するデータが生成され、共通制御装置に送信されるため、一般通信装置は新共通鍵を得ることが可能となり、新共通鍵の更新漏れを回避することができる。

[0111] (14)上記構成において、前記一般通信装置は、自機のステータスが前記配信完了である場合、前記前共通鍵と前記新共通鍵とにより受信データを復号化し、どちらの共通鍵で前記受信データが暗号化されたかを特定する復号化手段を更に備えることが好ましい。

[0112] この構成によれば、ステータスが配信完了である一般通信装置と、ステータスが移行中である一般通信装置とが混在する上記第2のネットワーク状態下において、ステータスが移行中である一般通信装置は、新共通鍵、或いは前共通鍵により暗号化された送信データを正確に復号化することができる。

[0113] (15)上記構成において、前記復号化手段は、自機のステータスが前記移行中である場合、前記前共通鍵と前記新共通鍵とを使用して前記受信データを復号化し、どちらの共通鍵で前記受信データが暗号化されたかを特定することが好ましい。

[0114] この構成によれば、ステータスが配信完了である一般通信装置と、ステータスが移行中である一般通信装置とが混在する上記第2のネットワーク状態下において、ステータスが移行中である一般通信装置は、新共通鍵、或いは前共通鍵を用いて暗号化された送信データを正確に復号化することができる。

[0115] (16)上記構成において、前記復号化手段は、自機のステータスが前記第2の更新完了である場合、前記新共通鍵を使用して受信データを復号化することが好ましい。

[0116] この構成によれば、上記第3のネットワーク状態下のステータスが更新完了である一般通信装置は、新共通鍵により新共通鍵を用いて暗号化された送信データを正確に

復号化することができる。

[0117] (17)本発明による一般通信装置は、ステータスが配信完了になった全ての一般通信装置に第1の状態遷移要求を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信する共通鍵制御装置に対して通信ネットワークを介して接続され、前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第1の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第2の状態遷移要求を受信したとき、ステータスを前記移行中から前記更新完了に戻す遷移手段と、ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、ステータスが前記更新完了にあるとき最新の共通鍵により送信データを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵を用いて送信データを暗号化する暗号化手段とを備えることを特徴とする。

[0118] (18)本発明による共通鍵制御装置は、複数の一般通信装置に対して通信ネットワークを介して接続された共通鍵制御装置であって、前記一般通信装置は、前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から配信完了に遷移させ、前記共通鍵制御装置から第1の状態遷移要求を受信したとき、ステータスを前記配信完了から移行中に遷移させ、前記共通鍵制御装置から第2の状態遷移要求を受信したとき、ステータスを移行中から更新完了に戻す遷移手段と、ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、ステータスが前記更新完了にあるとき最新の共通鍵により送信データを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵により送信データを暗号化する暗号化手段とを備え、全ての一般通信装置へ新共通鍵の更新要求を送信後に、新共通鍵更新応答を送信した全ての一般通信装置に第1の状態遷移要求

を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信することを特徴とする。

産業上の利用可能性

[0119] 本発明にかかる通信システムは、共通鍵の更新時においてシステム内で更新された共通鍵を保持する機器と、保持しない機器との間でも通信を行うことが可能となり、特にホームネットワークのようにM:Nのネットワークに適用した場合の効果が過大となる。また、本発明にかかる共通鍵制御装置を使用して共通鍵を管理すれば、リソースの小さな家電機器等の一般通信装置に対する効果が過大となる。

請求の範囲

[1] 更新前の前共通鍵を保持する複数の一般通信装置と、前記一般通信装置に対して所定のネットワークを介して接続され、前記前共通鍵を新共通鍵に更新する共通鍵制御装置とを備え、

前記共通鍵制御装置は、

ステータスが配信完了になった全ての一般通信装置に第1の状態遷移要求を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信するデータ送信処理手段を備え、

前記一般通信装置は、

前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第1の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第2の状態遷移要求を受信したとき、ステータスを前記移行中から前記更新完了に戻す遷移手段と、

ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、

ステータスが前記更新完了にあるとき、最新の共通鍵によりデータを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵を用いて送信データを暗号化する暗号化手段とを備えることを特徴とする通信システム。

[2] 前記共通鍵制御装置は、

前記新共通鍵を乱数により生成する共通鍵更新手段を更に備えることを特徴とする請求項1記載の通信システム。

[3] 前記共通鍵更新手段は、前記前共通鍵による送信データの暗号化回数又は受信データの復号化回数がある一定回数を越えた場合、前記新共通鍵を生成することを特徴とする請求項2記載の通信システム。

[4] 前記共通鍵更新手段は、前記前共通鍵による送信データの暗号化回数と受信データの復号化回数との和がある一定回数越えた場合、前記新共通鍵を生成すること

を特徴とする請求項2記載の通信システム。

[5] 前記共通鍵更新手段は、前記前共通鍵の使用期間が一定時間経過した場合、前記新共通鍵を生成することを特徴とする請求項2記載の通信システム。

[6] 前記共通鍵保持手段は、前記一般通信装置へ送信した共通鍵の履歴を保持し、送信した各共通鍵と、各共通鍵送信した前記一般通信装置のアドレスを含む一般通信装置情報とを対応づけて記憶する管理テーブルを保持することを特徴とする請求項1～5のいずれかに記載の通信システム。

[7] 前記共通鍵更新手段は、前記管理テーブルにより一般通信装置情報が記憶されていない一般通信装置からデータを受信した場合、新共通鍵を生成し、前記管理テーブルにより一般通信情報が記憶されている一般通信装置が保持する共通鍵を前記新共通鍵に更新することを特徴とする請求項6記載の共通鍵制御装置。

[8] 前記共通鍵制御装置は、

前記一般通信装置がネットワーク接続時において保持する初期共通鍵を入力するための初期共通鍵入力手段を更に備えることを特徴とする請求項1～7のいずれかに記載の通信システム。

[9] 前記初期共通鍵入力手段は、キーボード、タッチパネル、及びマウスのうちの少なくともいずれか1つを含むことを特徴とする請求項8記載の通信システム。

[10] 前記初期共通鍵入力手段は、初期共通鍵を保持する一般通信装置のリモコンと、前記リモコンからの信号を受け取る受光部とを含むことを特徴とする請求項8記載の通信システム。

[11] 前記初期共通鍵入力手段は、符号読取り装置であることを特徴とする請求項8記載の通信システム。

[12] 前記初期共通鍵入力手段は、記憶媒体駆動装置でることを特徴とする請求項8記載の通信システム。

[13] 前記一般通信装置は、

通信不可能状態から通信可能状態になったとき、前記共通鍵制御装置に対して新共通鍵の送信を要求するデータを作成し、前記共通鍵制御装置に送信する共通鍵要求手段を更に備えることを特徴とする請求項1～12のいずれかに記載の通信シス

テム。

[14] 前記一般通信装置は、

自機のステータスが前記配信完了である場合、前記前共通鍵と前記新共通鍵とにより受信データを復号化し、どちらの共通鍵で前記受信データが暗号化されたかを特定する復号化手段を更に備えることを特徴とする請求項1～13のいずれかに記載の通信システム。

[15] 前記復号化手段は、自機のステータスが前記移行中である場合、前記前共通鍵と前記新共通鍵とを使用して前記受信データを復号化し、どちらの共通鍵で前記受信データが暗号化されたかを特定することを特徴とする請求項14記載の通信システム。

[16] 前記復号化手段は、自機のステータスが前記更新完了である場合、前記最新の共通鍵を使用して受信データを復号化することを特徴とする請求項14又は15記載の通信システム。

[17] ステータスが配信完了になった全ての一般通信装置に第1の状態遷移要求を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信する共通鍵制御装置に対して通信ネットワークを介して接続され、

前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第1の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第2の状態遷移要求を受信したとき、ステータスを前記移行中から前記更新完了に戻す遷移手段と、

ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、

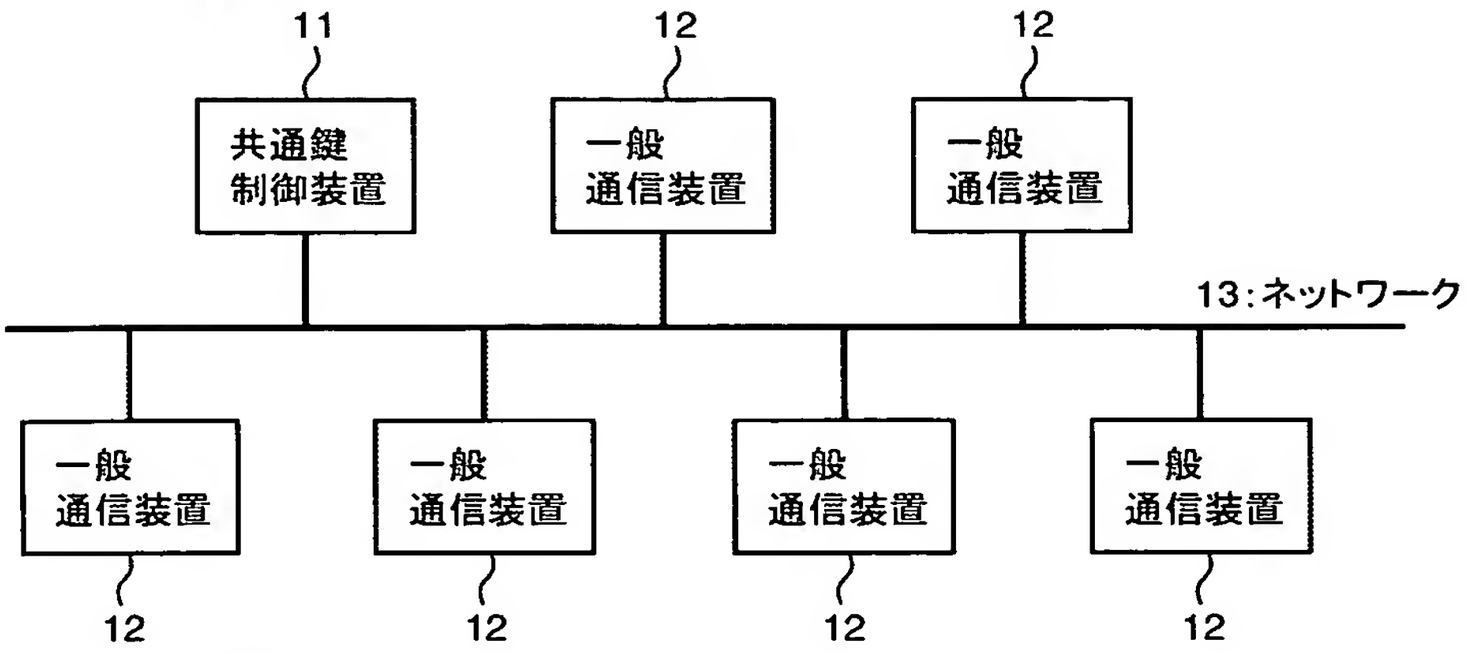
ステータスが前記更新完了にあるとき最新の共通鍵により送信データを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵を用いて送信データを暗号化する暗号化手段とを備えることを特徴とする一般通信装置。

[18] 複数の一般通信装置に対して通信ネットワークを介して接続された共通鍵制御装置であって、

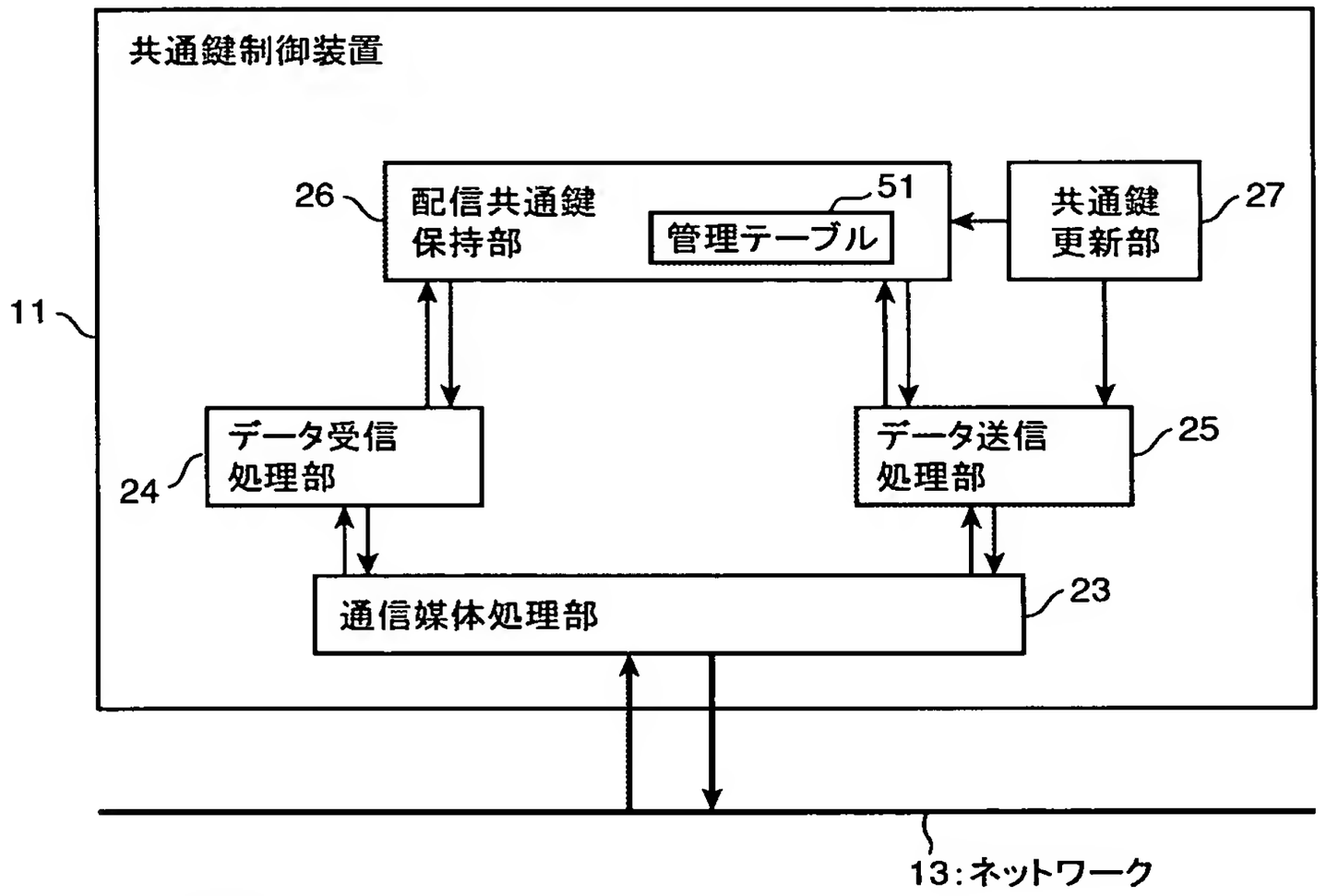
前記一般通信装置は、前記共通鍵制御装置から新共通鍵を受信したとき、ステータスを更新完了から配信完了に遷移させ、前記共通鍵制御装置から第1の状態遷移要求を受信したとき、ステータスを前記配信完了から移行中に遷移させ、前記共通鍵制御装置から第2の状態遷移要求を受信したとき、ステータスを移行中から更新完了に戻す遷移手段と、ステータスが前記更新完了にあるとき、最新の共通鍵のみを保持し、ステータスが前記配信完了及び前記移行中にあるとき、前記前共通鍵と前記新共通鍵とを共に保持する共通鍵保持手段と、ステータスが前記更新完了にあるとき最新の共通鍵により送信データを暗号化し、ステータスが前記配信完了にあるとき、前記前共通鍵により送信データを暗号化し、ステータスが前記移行中にあるとき、前記新共通鍵により送信データを暗号化する暗号化手段とを備え、

全ての一般通信装置へ新共通鍵更新要求を送信後に、新共通鍵更新応答を送信した全ての一般通信装置に第1の状態遷移要求を送信し、全ての一般通信装置に新共通鍵を配信することができたとき、全ての一般通信装置に第2の状態遷移要求を送信することを特徴とする共通鍵制御装置。

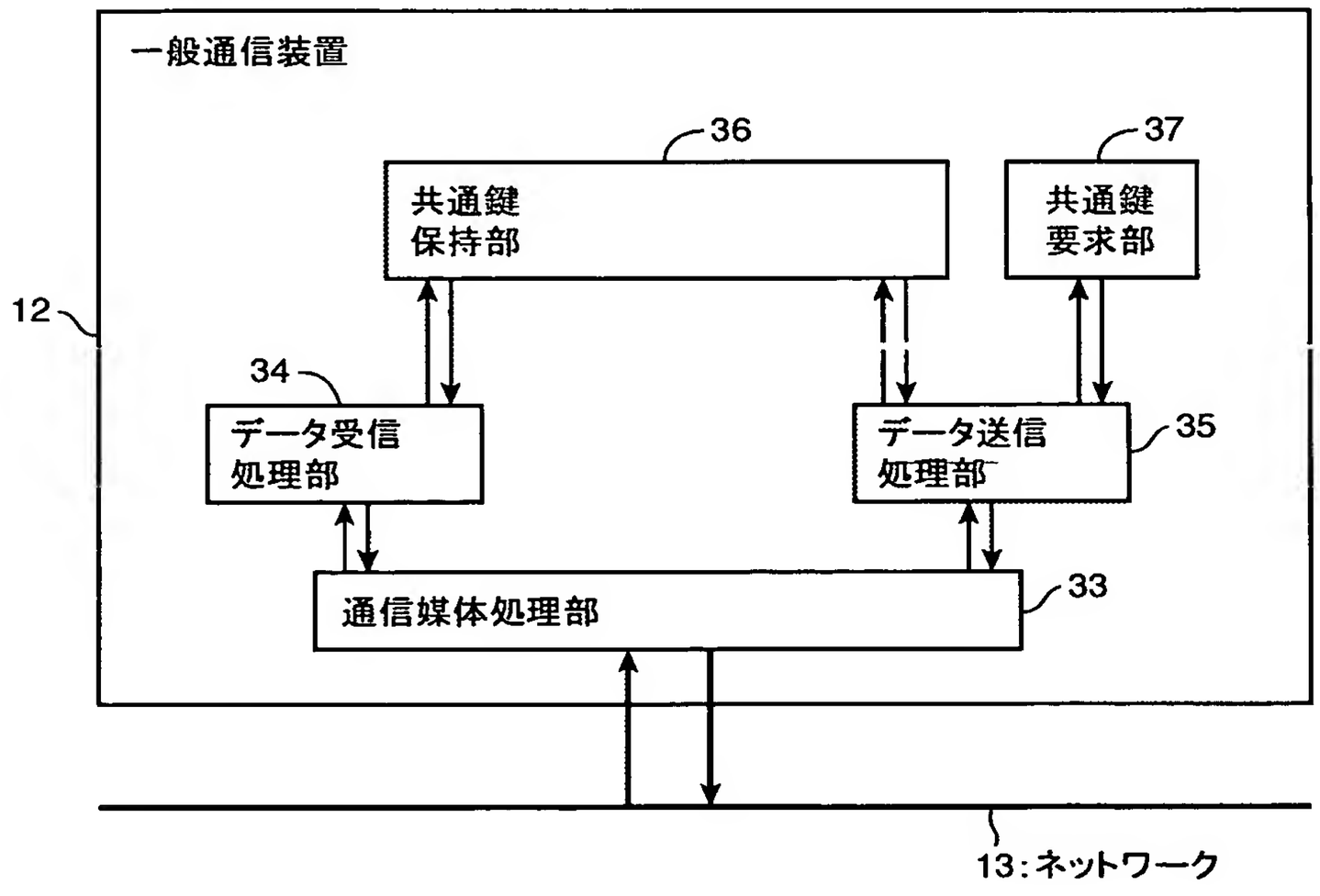
[図1]


11
12
12
共通鍵
制御装置
一般
通信装置
一般
通信装置
13:ネットワーク
一般
通信装置
一般
通信装置
一般
通信装置
一般
通信装置
12
12
12
12

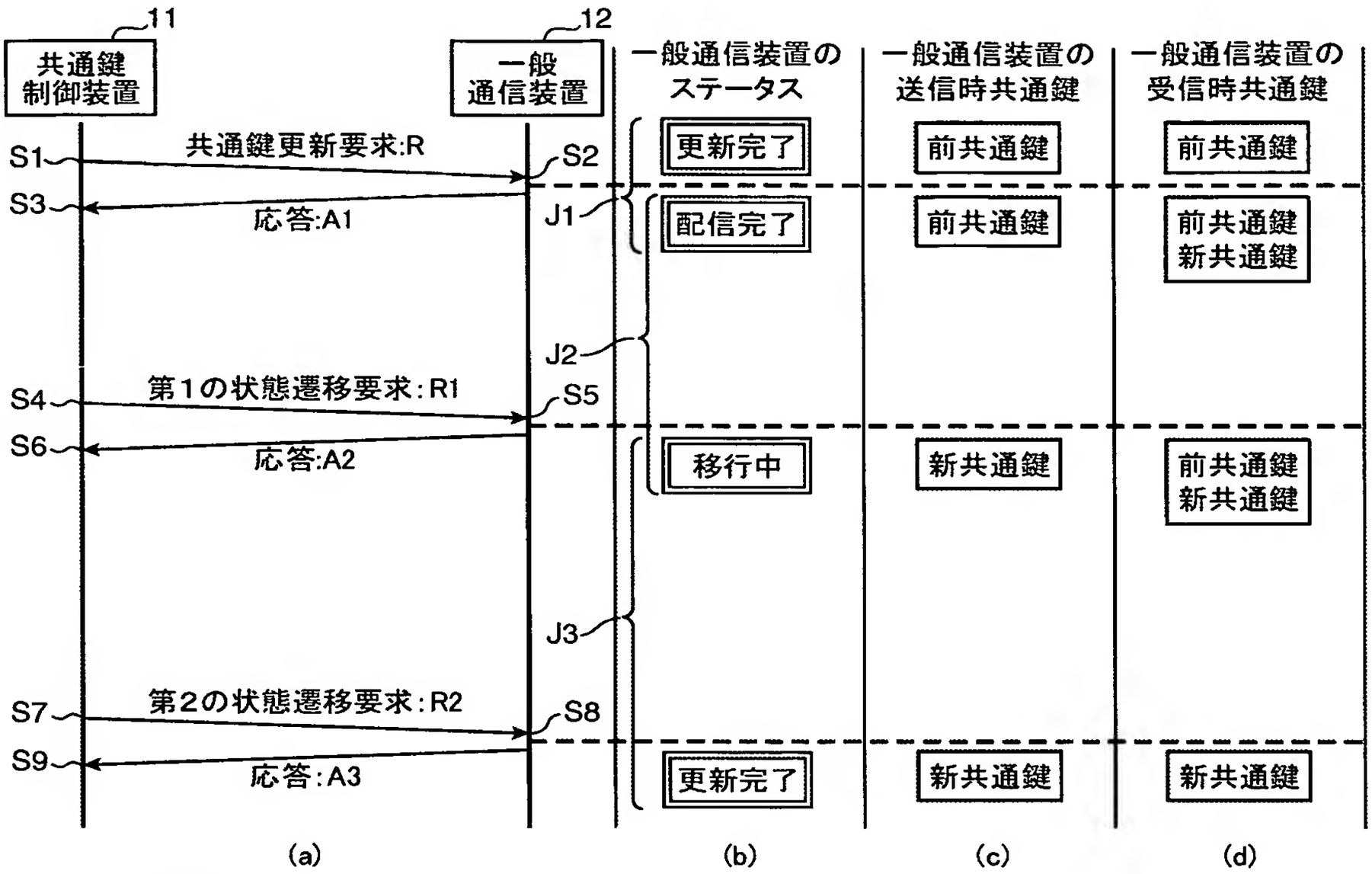
[図2]


共通鍵制御装置
26
配信共通鍵
保持部
51
管理テーブル
共通鍵
更新部
27
11
データ受信
処理部
24
データ送信
処理部
25
通信媒体処理部
23
13:ネットワーク

[図3]


一般通信装置
36
共通鍵
保持部
37
共通鍵
要求部
12
34
データ受信
処理部
データ送信
処理部
35
通信媒体処理部
33
13:ネットワーク

[図4]

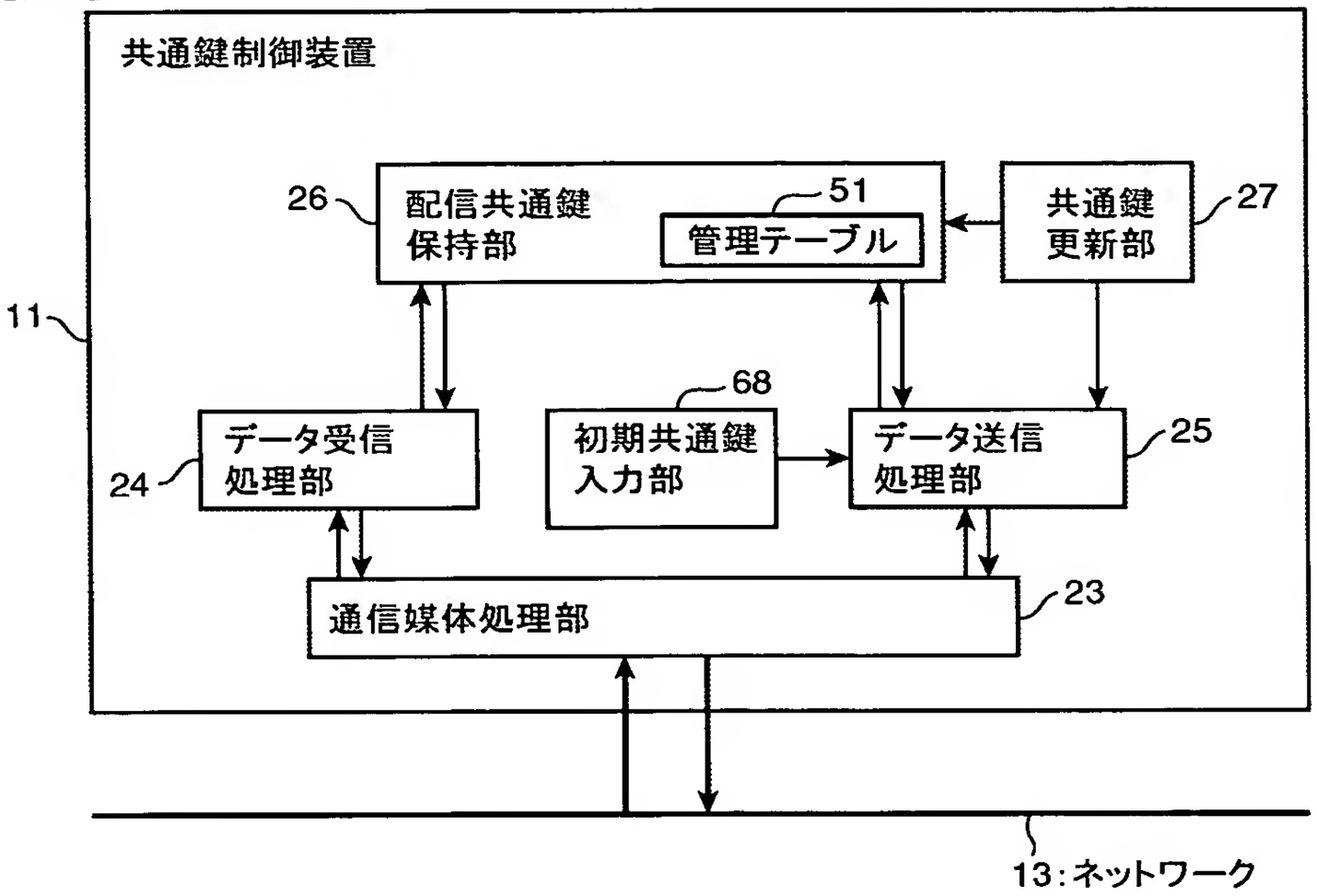


[図5]

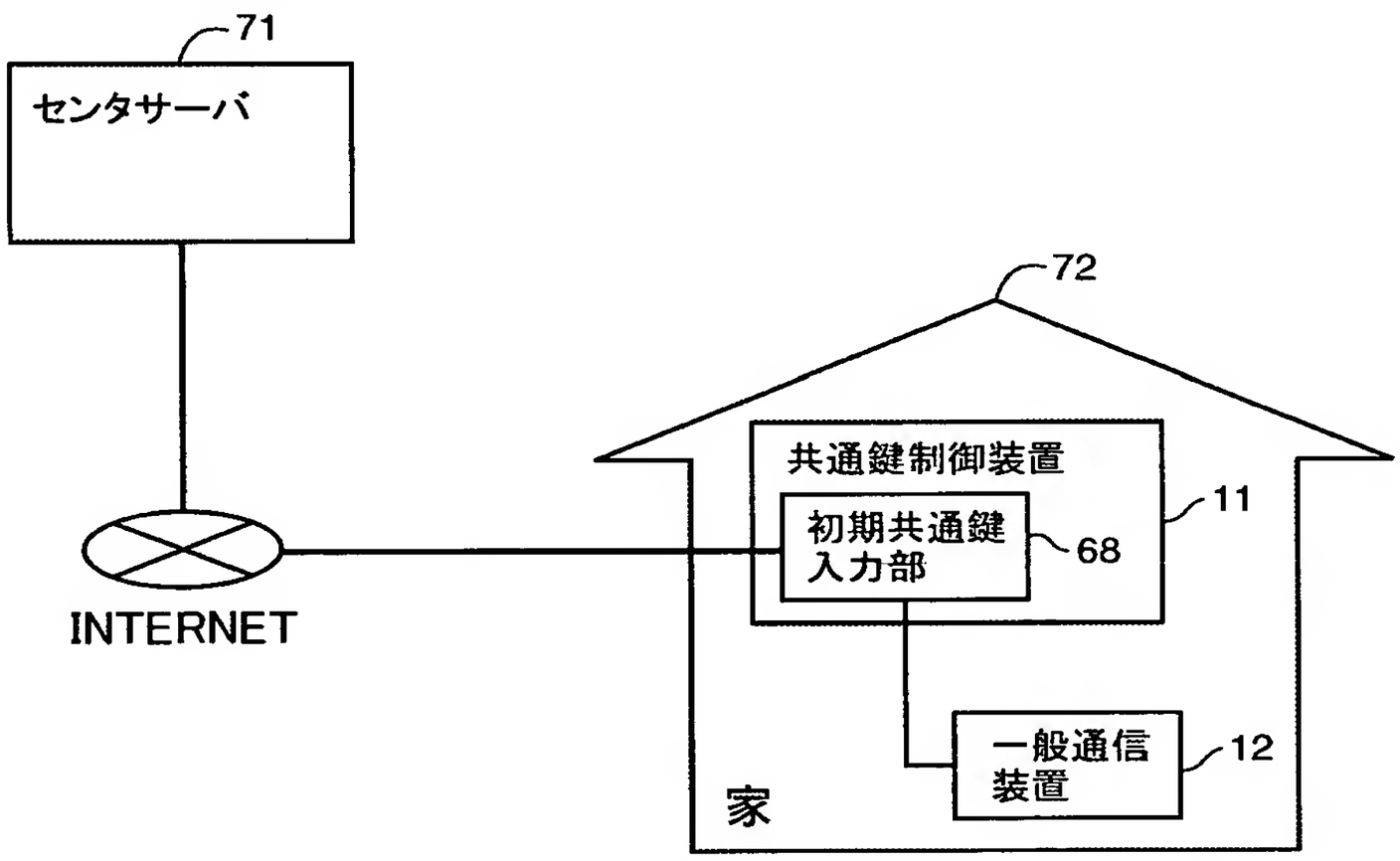
51

共通鍵	配信先アドレス
最新共通鍵	アドレスA、アドレスB、アドレスC、…
共通鍵 1	アドレスD
共通鍵 2	アドレスE、アドレスF
共通鍵 4	アドレスG
⋮	⋮
共通鍵 n	アドレスT

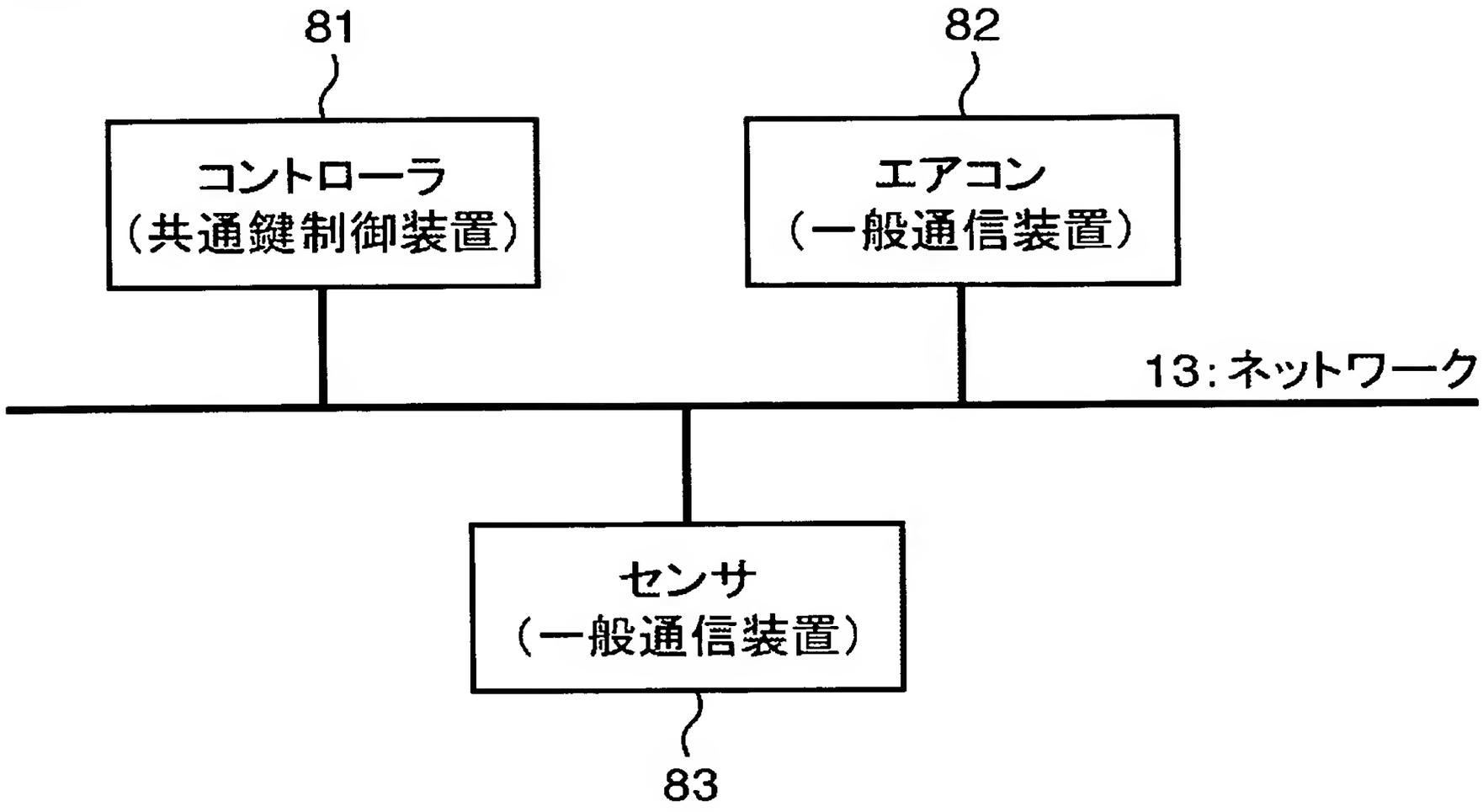
[図6]


共通鍵制御装置
26
配信共通鍵
保持部
51
管理テーブル
共通鍵
更新部
27
11
68
データ受信
処理部
24
初期共通鍵
入力部
データ送信
処理部
25
通信媒体処理部
23
13:ネットワーク

[図7]


71
センタサーバ
72
共通鍵制御装置
初期共通鍵
入力部
68
11
INTERNET
一般通信
装置
12
家

[図8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/007894

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-239125 A (Nippon Telegraph And Telephone Corp.), 31 August, 1999 (31.08.99), Par. No. [0044]; Fig. 1 (Family: none)	1-18

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 27 July, 2005 (27.07.05)	Date of mailing of the international search report 16 August, 2005 (16.08.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２００５／００７８９４

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L9/08

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 11-239125 A（日本電信電話株式会社）1999.08.31, 【0044】段落、図１（ファミリーなし）	1-18

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２７．０７．２００５	16.8.2005

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	中里　裕正	５Ｓ	３５７４
	電話番号　０３－３５８１－１１０１　内線　３５４６		